

Rec'd Bauer

MULTI-SYSTEM DATA TERMINAL DESIGN

USING AUTHENTICATORS

R.K. Bauer

1. INTRODUCTION

Often Government personnel require access to multiple EDP systems, each classified at a different level. Use of separate terminal equipment for each system is inefficient, expensive and often leads to an explosion of terminals and interconnecting cables. Use of a single terminal, while more convenient, poses the danger of information spillage. Classified information may still be present within the terminal when it is connected to an unclassified EDP host after a classified work session. This problem is of concern for terminals which include internal storage and especially for those which incorporate permanent storage media such as disks, tapes and nonvolatile memory. Currently these terminals must be "sanitized" after use in a classified environment in order to completely expunge any classified information residue. Such sanitization procedures are inconvenient, make demands upon the operator and require trust in their correct function.

Rather than ban the use of storage terminals, a solution is sought which not only allows their use, but exploits their storage features. It is convenient for such terminals to perform a data transfer function. Information selected from an unclassified system is stored within the terminal and later transferred onto a classified system to aid work performed there. Selective information transfer to systems at the same or higher classification level is a distinct advantage and represents no security risk. However the reverse of this process represents information downgrade or compromise, and must be prevented.

This paper describes a solution approach based upon data marking with authenticators. The approach utilizes special marking and filtering devices and specialized terminals which isolate the keyboard from the display, local memory, storage and computation facilities. The design makes extensive use of hardware security features and is far less complicated (and more trustworthy) than solutions employing multilevel secure operating systems in the terminal.

2. DATA MARKING AND FILTERING

Markers and filters are interposed between all EDP equipment and the communications medium which they use for intercommunication. The markers indelibly mark data packet classification level prior to their entry into the communications medium. The filters effectively block high level data which their host may not view. The communications medium underlying the markers and filters may be point-to-point cabling, a local area network, or even a satellite link. Its exact nature is unimportant, only that it is certified to carry the highest level of classified information presented by any attached host EDP system. The markers and filters must also be protected at this level.

Figure 1 shows two EDP hosts operating at different security levels and a terminal which may access either host. Data which leaves either EDP host is labeled with its classification level by the attached marker. To ensure that the label and data will not be altered, it is sealed with an authenticator. This guarantees to the receiving filter that the packet and its level are authentic and have not been altered or otherwise manipulated during transit or storage. The authenticator is a cryptographic tag computed over the entire data packet contents and its level, based upon a secret key. The process is analogous to encryption, but rather than producing scrambled data, produces the authenticator. The authenticator can be validated by any filter having the correct key. Any single bit alteration in the data, level or key will produce a drastically different authenticator. Algorithms suitable for encryption are easily used for this purpose. DES in cipher block chaining mode is used by the RECON Guard, although stronger algorithms are as easily employed.

Filters are able to recalculate the authenticator for data packets presented to them using the secret key and levels which it stores. It notes if it is authorized for the classification level indicated by the label in the data packet, recomputes the authenticator using the key and compares the result with the original authenticator appended on the data packet. If they match the data is passed, otherwise it is blocked. The level and authenticator on acceptable data packets can either be stripped or left intact by the filter as is convenient. If any of the following conditions exist, the data packet is not passed:

1. The filter is not authorized for the classification level indicated by the data packet.
2. The data in the data packet was altered
3. The classification level marking in the data packet was altered
4. The authenticator in the data packet was altered
5. The data packet authenticator is absent

Point 1 is the means by which viewing rights are controlled. Unlike the marker, the filter may accommodate several

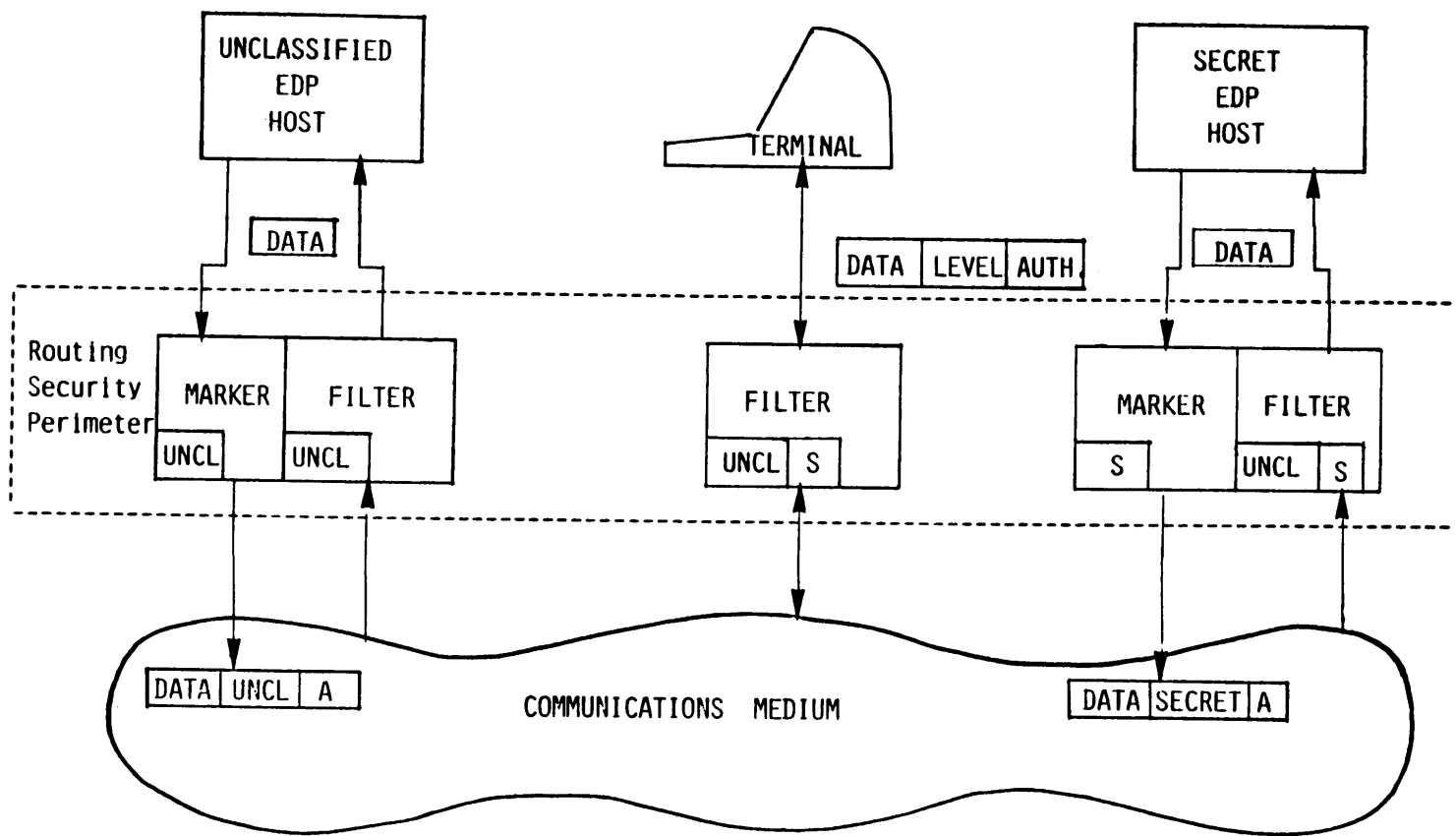


FIGURE 1: DATA PACKET MARKING & FILTERING

classification level/key pairs depending upon the EDP host's viewing rights. For example, a Top Secret host may have keys for Unclassified, Confidential, Secret and Top Secret allowing it to view data packets with any of these markings. Points 2-4 represent inadvertent or intentional tampering with the data packet during transmission or storage in the terminal. All such tampering is detected (barring cryptanalysis of the authenticator calculation algorithm or key compromise) and data packet delivery prevented. Point 5 covers loss of authenticator and misrouted information from the communications medium. It is also useful for designating unreleasable data packets.

We will now explain how data can be moved from the Unclassified EDP host to the Secret Host and how reverse movement is blocked. The terminal establishes a session with the Unclassified EDP host and attempts to move data into the terminal storage. This is successful. The marker marks the data Unclassified, and the terminal filter is authorized at that level. The terminal filter leaves the level and authenticator intact, protecting the data and level from undetectable alteration while within the terminal. The terminal now establishes a session with the Secret EDP host and attempts to forward the data. This also is successful. The terminal filter forwards the outbound packet without examination or modification. Any discrepancies are detected by the Secret host's filter upon receipt of the data packet. Alternately, the terminal may have a direct, outbound only connection to the communications medium for this purpose. The outbound only requirement stems from the need to filter all incoming data packets to the terminal.

Similarly Secret data can be moved, with level markings and authenticators intact, into the terminal. However, this data cannot be exported to the Unclassified system because it will be blocked by the Unclassified host filter which is not authorized at that level. If the terminal operator alters the level in the packet, the filter would block transmission as the authenticator would be incorrect. Similar manipulations are also detected by changes in authenticator.

3. TERMINAL DATA ENTRY

Unfortunately there is an additional complication not covered by Figure 1. This is the issue of new data entry at the terminal. The difficulty is in determining the proper level at which the terminal marker(s) should operate. Some terminal data entry is essential if for no other reason than to issue logon sequences for the various EDP hosts, formulate data base queries, enquire concerning query status etc. Obviously such information must be unclassified when directed to an unclassified system, but may contain sensitive information when queries are directed to a classified system. For some applications it may be possible to use "canned" logon sequences and queries with precalculated

authenticators. However this is an application specific solution, greatly restricts operator flexibility and invariably leads to future alteration. Another application specific approach uses markers which can recognize data at different classification levels. This rather unsatisfactory solution requires rigidly controlled formats, a great deal of trust in software correct function, and has little flexibility.

Most generalized approaches rely upon the operator to correctly label keyboard entered data. Approaches differ in the degree of operator support provided and in the level of operator trust. The approach illustrated in Figure 2 allows the operator to switch select the classification level of data entered, which has interesting sanitization implications.

The keyboard is memoryless and strongly isolated from the rest of the terminal. This eliminates the need for sanitization when the operator switches from a higher to lower classification marking. Through a user selectable control sequence, the keyboard may instruct the local computer or send control information onto the communications medium. The keyboard controller module is responsible for directing keystrokes to the local computer or marker as specified by the user. It also prevents transfer of data (classified or otherwise) from the local computer into the keyboard subsystem. Keystrokes destined for the marker and remote hosts are directed to the dedicated marker where they are labeled according to the operator selected switch position. These packets are sealed with an authenticator prior to transmission.

The terminal computer and display subsystem connects to the communications medium via its own filter which allows it to receive and forward data packets. Incoming data packets from the communications medium are screened to ensure they are viewable by the terminal. Incoming data packets passed by the filter have their level markings and authenticator intact. These marked packets may be stored, processed or displayed as specified by the operator via the keyboard, and otherwise intermixed with unmarked and unsealed data. Data directed from the display subsystem to a remote host is forwarded by the filter without examination or modification to the communications medium. However the display subsystem and filter have no provisions for marking packet level or appending authenticators. Therefore only previously marked and sealed data received by the terminal can be delivered to its destination. Only these packets will have correct authenticators and be passed by remote host filters.

Depending upon the communications interface, multiple simultaneous connections can be supported, even to EDP hosts running at different security levels. Since the operator must correctly label the security level of keyboard entered data, all displayed data must be clearly marked with its classification level. Visual segregation of multilevel data is readily accomplished via separate display windows, colors, or type fonts for each

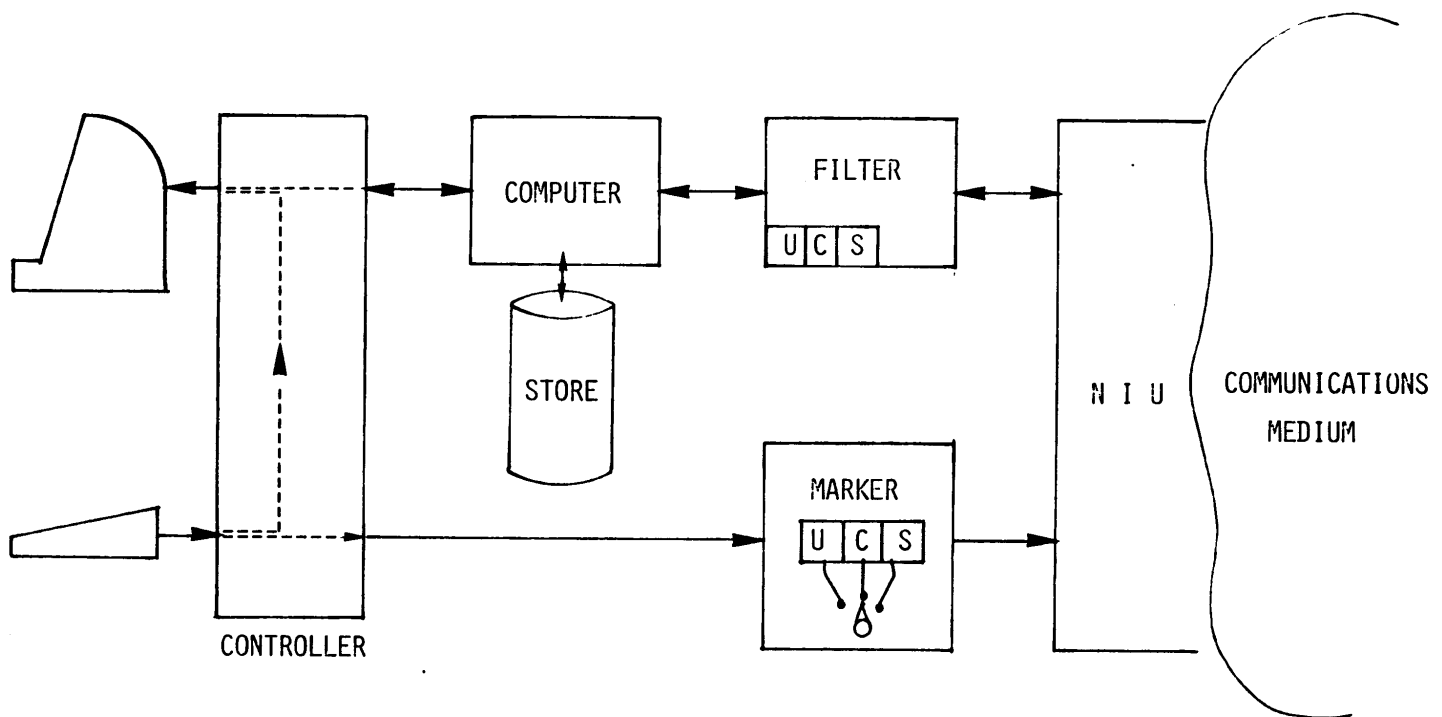


FIGURE 2: TERMINAL BLOCK DIAGRAM WITH KEYBOARD INPUT
MARKED AT OPERATOR-SELECTED LEVEL

different level. Equally important is correct and complete display of classified information. Obviously, inaccurate display of data and its sensitivity level might confuse the operator, causing improper marking of keyboard entered data. This condition is true even when only single level is displayed, making display hardware and software security relevant.

4. IMPLEMENTATION CONSIDERATIONS

The previous sections raised substantial security requirements which are levied upon the terminal architecture and subsystems in addition to normal functional requirements. These security requirements affect terminal design as strongly as functional requirements and influence make/buy decisions. This section traces further the impact of security upon terminal implementation. Implementation impacts of terminal keyboard and display requirements are discussed followed by a discussion of the marker/filter implementation.

4.1 Terminal Considerations

A major requirement is suitable isolation of the keyboard and display subsystems. Recall that all outbound keyboard input is labeled and sealed according to the classification level switch position. Restricting this to keyboard input not only limits the rate at which data might be compromised but makes a clear impression as to the source of data so labeled. The best isolation is accomplished in hardware by completely separating the circuitry for the two subsystems. Suitable "one-way" communication between the two subsystems could be implemented by a specific hardware protocol. Verification of correctness is accomplished by design review and inspection of actual hardware circuit board traces.

Accurate and complete display of classified information is another important issue. The display software and hardware must be able to recognize data packet format, extract the appropriate classification level label, and accurately display all the data in the packet in the appropriate color, font or in the appropriate window. Isolation of this functionality from the general local computer is important to ease verification of these properties, giving rise to the special controller module shown in Figure 2. This controller hardware directly controls the physical aspects of the display and is programmable. The display control software must be verified to properly manipulate the hardware in response to commands to display classified data.

Most of the other terminal requirements center upon the support of and interface to the marker/filter subsystem. Because markers and filters must be protected to the same extent as the communications medium, it is desirable to physically co-locate them. In this approach the terminal must support communications to a marker/filter subsystem which is not necessarily located next to,

or within the terminal enclosure. These communications must provide a trusted path over which the terminal may set the marking level in the marker. Alternately the marker and terminal can be co-located. This eases the interface chores between the terminal and marker and allows switch selection of marking level. However the marker must be secured and will likely require a special enclosure.

4.2 Marker/Filter Subsystem Considerations

This subsystem is the heart of the approach and embodies little risk due to extensive experimentation conducted during the RECON Guard program. This program resulted in the implementation and security verification of a prototype marker/filter system for use in the RECON environment. Evaluation of its suitability for protecting sensitive RECON data base records while providing common network access to others has been successfully completed.

This prototype equipment is well adapted for use in this application. Each filter or marker is implemented by three separate processing environments, each supported by its own microprocessor. Two microprocessors independently interface to the protected data base machine and the network communications processor. The third microprocessor performs all security processing. The security processor is supported by an encryption peripheral which computes authenticators based upon the secret keys it stores. The hardware design ensures all high to low data transfer is mediated by the security processor. The simplicity of the security task, freedom from interface concerns and software verification ensure that the security processor software is correct and secure.

5. A. PRACTICAL APPLICATION

The ideas in the previous sections solve an immediate problem. Government intelligence analysts often draw upon a variety of EDP systems to prepare intelligence reports. While the analyst's primary EDP system may be highly classified, a wide range of less restricted supportive material may be available at other agencies which would be of tremendous value in report preparation. As an extreme example, dial up access to unclassified medical and/or newspaper data bases is useful. The goal is to allow information extraction from these other sources while maintaining complete confidence that classified data within the terminal is not leaked during the connection.

Figure 3 shows a configuration of networks, hosts, terminals, markers and filters which support this application. Local agency resources (Hosts A&B and terminals a&b) are interconnected via a local area network. The local agency network is connected to an interagency network, allowing connection to Host D at another agency and connection to a dial-out modem for accessing an

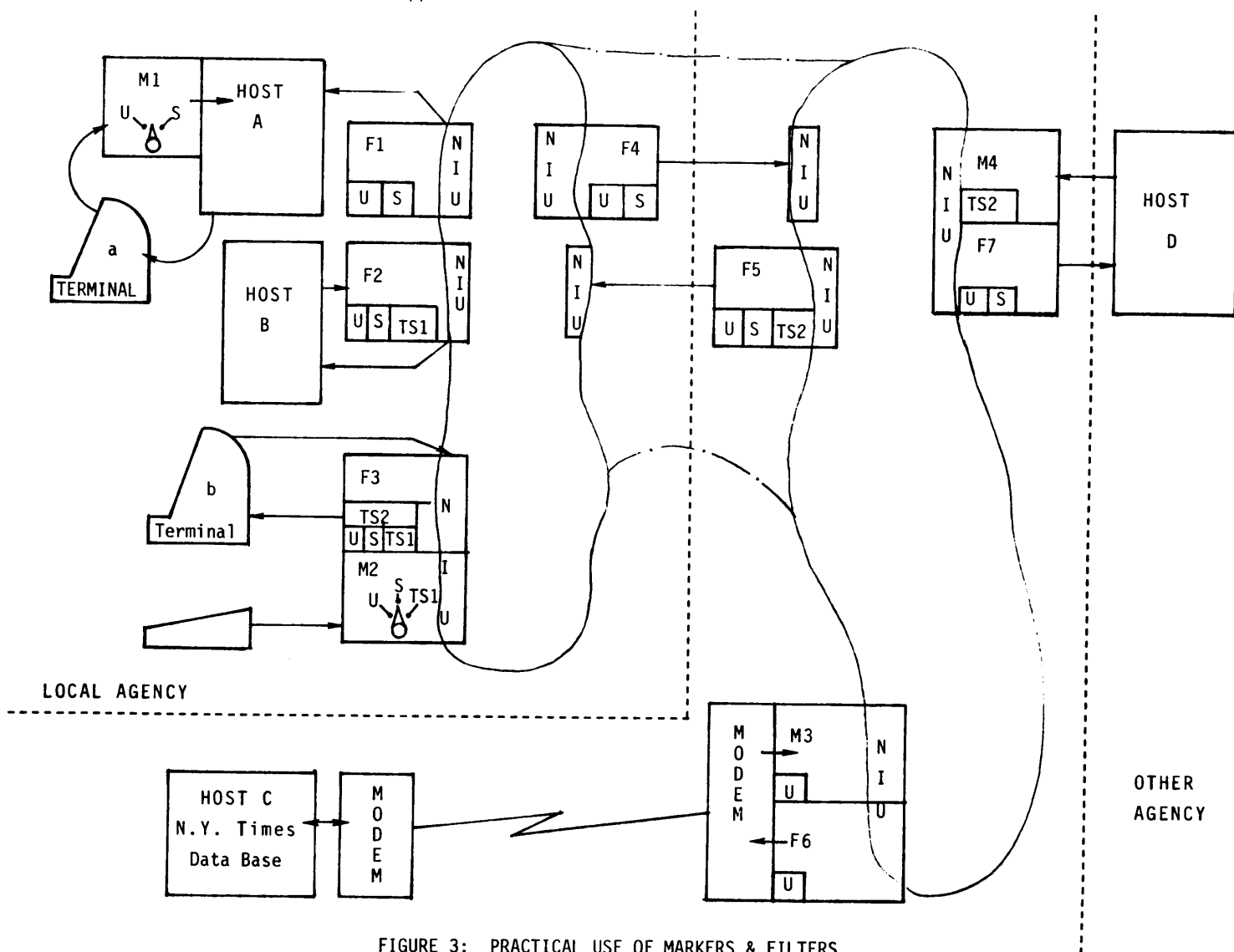


FIGURE 3: PRACTICAL USE OF MARKERS & FILTERS

unclassified data base.

Table I describes viewing, forwarding and creation rights for the different hosts and terminals in Figure 3. The first table column (MAY VIEW OR STORE) lists the level of packets which may be input and optionally stored by the host or terminal. In our example there are five categories of data packet: unclassified (U), secret (S), top secret category 1 (TS1), top secret category two (TS2), and unmarked, which is data with no level marking or authenticator.

Table I: Host and Terminal Capabilities for Figure 3

DEVICE	MAY VIEW OR STORE	MAY FORWARD	MAY CREATE
Term a	U,S,TS1,TS2, unmarked	-	U,S (M1)
Term b	U,S,TS1, TS2, (F3)	U,S,TS1,TS2	U,S,TS1 (M2)
Host A	U,S,TS1,TS2, unmarked	U,S, (F1)	-
Host B	U,S,TS1,TS2, unmarked	U,S,TS1 (F2)	-
Host C	U (F6)	-	U (M3)
Host D	U,S (F7)	-	TS2 (M4)

The second column details forwarding capabilities. Terminals and hosts with direct outbound connections to a network may release or forward any data they contain. Data packet forwarding by terminals and hosts whose outbound connections are mediated by a filter is limited to appropriately marked data packets. Finally the last column shows data packet marking or creation capabilities. Only markers can mark and seal a data packet. Some markers apply a fixed level, others allow the operator to select the marking level. Throughout the table, filter and marker identifiers in parenthesis show which marker or filter is active in supplying a capability or imposing a restriction.

Filters four and five do not appear in table I and could be removed in some instances as shown by the long dashed line in Figure 3. They are introduced to provide a greater degree of local control and security confidence. The short dashed line delineates local "zones of control." Filter 4, under the local agency's physical control, provides a high degree of confidence that only unclassified and secret data will be allowed to leave

the local agency. The filter in this configuration closely resembles the RECON guard.

Consider a connection between Terminal b and Host D at the other agency. Even though Terminal b can view all data and can even create Top secret data restricted to the local agency (TS1), filter F4 allows only unclassified and secret transmissions to host D. On the other hand all data contained in host D is releasable and is marked TS2 by M4 which is passed by filters F5 and F3 allowing its use by the terminal. TS2 marked data could then be forwarded by the terminal to either of its local hosts during a later connection.

As a second example, consider a connection between Terminal b and Host C, the New York times data retrieval system. Retrieved information is marked unclassified by M3 and released by F5 and F3. Queries from terminal b are marked unclassified by M2 with its switch in the U position. Queries thus marked are released by F4 and F6 before they are received by Host C. Should the operator mistakenly set the terminal marker to secret (S), the query would be blocked by F6. Similarly a missetting at TS1 would be blocked by F4. Marked data released from terminal B's computer/display unit would be similarly filtered. Unmarked data from the computer/display would be blocked by F4.

6. CONCLUSION

Practical solution of the multi-system terminal problem is possible using authenticators. Data is permanently marked as to its classification level and released only to systems with the appropriate viewing rights. Terminals may communicate with and view data from several systems operating at different security levels simultaneously. Solution implementation maximizes use of existing terminal equipment and capitalizes on readily available security technology, to yield a low risk, near term solution approach.